JOURNAL OF COMBINATORIAL THEORY (A) **18**, 149–164 (1975)

On Hadamard Matrices

JENNIFER SEBERRY WALLIS

Department of Mathematics, I.A.S., Australian National University, Canberra, Australia

Communicated by Marshall Hall, Jr.

Received February 14, 1974

Recent advances in the construction of Hadamard matrices have depended on the existence of Baumert–Hall arrays and four (1, −1) matrices A, B, C, D of order m which are of Williamson type, that is pairwise satisfy

(i) $MN^T = NM^T$ and

(ii) $AA^T + BB^T + CC^T + DD^T = 4mI_m$.

If (*i*) is replaced by (*i'*)$MN = NM$ we have Goethals–Seidel matrices. These matrices are very important to the determination of the Hadamard conjecture: *that there exists an Hadamard matrix of order 4t for all natural numbers t.*

This paper shows how the Williamson type and Goethals–Seidel type Hadamard matrices may be combined by introducing F-matrices which are a generalization of both Williamson and Goethals–Seidel matrices. Several constructions for F-matrices are given showing they exist for the new orders 119, 171, 185, 217 and the new classes $\frac{1}{4}q(q+1)$, $q \equiv 3 \pmod 8$ a prime power and $\frac{1}{2}p(p-3)$, $p \equiv 1 \pmod 4$ and $p - 4$ both prime powers (among others).

1. Introduction and Basic Definitions

A matrix with every entry $+1$ or -1 is called a $(1, -1)$-*matrix*. An *Hadamard matrix* $H = (h_{ij})$ is a square $(1, -1)$ matrix of order n which satisfies the equation

$$HH^T = H^TH = nI_n .$$

We use J for the matrix of all 1's and I for the identity matrix. The Kronecker product is written $\times$.

A *Baumert–Hall array* of order t is a $4t \times 4t$ array with entries A, $-A$, B, $-B$, C, $-C$, D, $-D$ and the properties that:

(i) in any row there are exactly t entries $\pm A$, t entries $\pm B$, t entries $\pm C$, and t entries $\pm D$; and similarly for columns;

(ii) the rows are formally orthogonal, in the sense that if $\pm A$, $\pm B$, $\pm C$, $\pm D$ are realised as elements of any commutative ring then the distinct rows of the array are pairwise orthogonal; and similarly for columns.

The Baumert–Hall arrays are a generalisation of the following array of Williamson:

$$\begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix},$$

which gives, when A, B, C, D are replaced by matrices of *Williamson type*—that is $(1, -1)$ matrices of order m which pairwise satisfy

(i) $MN^T = NM^T$ and

(ii) $AA^T + BB^T + CC^T + DD^T = 4mI_m$,

an Hadamard matrix of order $4m$.

The status of knowledge about Williamson matrices and Baumert–Hall arrays is summarised below; these, together with the following theorem, give many infinite families of Hadamard matrices.

THEOREM 1 (Baumert and Hall). *If there exists a Baumert–Hall array of order t and a Willimson matrix of order m then there exists an Hadamard matrix of order $4mt$.*

Statement 1. There exist Baumert-Hall arrays of order

(i) $\{3, 5, 7, \ldots, 59, 61\} = B$,

(ii) $\{1 + 2^a \cdot 10^b \cdot 26^c : a, b, c \text{ natural numbers}\} = A$,

(iii) $5b$, $b \in A \cup B$.

(iv) $2n$, where $4n$ is the order of any Hadamard matrix,

(v) $(p^r + 1)t$, $p^r(p^r + 1)t$ where t is the order of any Baumert–Hall array and $p^r \equiv 1 \pmod 4$ is a prime power.

Statement 2. There exist Williamson type matrices of order

(i) $\{1, 3, 5, 7, \ldots, 29, 37, 43\}$,

(ii) $\frac{1}{2}(p + 1)$, $p \equiv 1 \pmod 4$ a prime power,

(iii) 9^d, d a natural number,

(iv) $\frac{1}{2}p(p + 1)$, $p \equiv 1 \pmod 4$ a prime power,

(v) $s(4s + 3)$, $s(4s - 1)$, $s \in \{1, 3, 5, \ldots, 25\}$,

(vi) 93,

(vii) $2n$, where n is the order of Williamson type matrices.

(viii) $2s(4s + 1), 4s + 1$ a prime power, $s \in \{1, 3, 5, ..., 25\}$,

(ix) $(p + 1)(p + 2), p \equiv 1 \pmod 4$ a prime power, $p + 3$ the order of a symmetric Hadamard matrix,

(x) others with more restrictive conditions.

See [2–4, 6–9] for details.

This leaves the following orders less than 100 for which Williamson type matrices are not yet known: 35, 39, 47, 53, 59, 65, 67, 70, 71, 73, 77, 83, 89, 94.

Let V be an additive abelian group of order v with elements $g_1, g_2, ..., g_v$.

Let $S_1, S_2, ..., S_n$ be subsets of V containing $k_1, k_2, ..., k_n$ elements, respectively. Write T_i for the totality of all differences between elements of S_i (with repetitions), and T for the totality of elements of all the T_i. If T contains each nonzero element a fixed number of times, λ say, then the sets $S_1, S_2, ..., S_n$ will be called $n - \{v; k_1, k_2, ..., k_n; \lambda\}$ *supplementary difference sets*. If $n = 1$ we have a (v, k, λ) *difference set* which is *cyclic* or *abelian* according as V is cyclic or abelian.

The type 1 $(1, -1)$ incidence matrix $M = (m_{ij})$ of order v of a subset X of V is defined by

$$m_{ij} = \begin{cases} +1 & g_j - g_i \in X, \\ -1 & \text{otherwise;} \end{cases}$$

while the type 2 $(1, -1)$ incidence matrix $N = (n_{ij})$ of order v of a subset Y of V is defined by

$$n_{ij} = \begin{cases} +1 & g_j + g_i \in Y, \\ -1 & \text{otherwise.} \end{cases}$$

It is shown in [9] that if M is a type 1 $(1, -1)$ incidence matrix of order v and N is a type 2 $(1, -1)$ incidence matrix of order v, $MN^T = NM^T$; while if M and N are both type 1 of order v, $MN = NM$.

If V is cyclic then a type 1 matrix is called *circulant* and a type 2 matrix is called *back-circulant*; i.e., $M = (m_{ij})$ satisfies

$$m_{1,j+1} = m_{i,j+i} \quad \text{and} \quad m_{1,j} = m_{1+i,j+i},$$

respectively.

Also in [9], it is shown that $R = (r_{ij})$ of order v, defined on V by

$$r_{i,j} = \begin{cases} 1 & \text{if } g_i + g_j = 0, \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

then if M is type 1, MR is type 2.

Hence if M and N are type 1 of order v, $MN = NM$ and $M(NR)^T = (NR)M^T$.

Further, if M_i, N_i are type 1 of order v_i and R_i is the appropriate matrix, given by (1), for v_i

$$(M_1 \times M_2 \times \cdots \times M_n)(N_1 \times N_2 \times \cdots \times N_n) = (N_1 \times N_2 \times \cdots \times N_n)(M_1 \times M_2 \times \cdots \times M_n)$$

and

$$(M_1 \times M_2 \times \cdots \times M_n)[(N_1 \times N_2 \times \cdots \times N_n)(R_1 \times R_2 \times \cdots \times R_n)]^T = [(N_1 \times N_2 \times \cdots \times N_n)(R_1 \times R_2 \times \cdots \times R_n)](M_1 \times M_2 \times \cdots \times M_n)^T.$$

We will call four (0, 1, −1) matrices X_1, X_2, X_3, X_4 of order x which satisfy

(i) $X_i * X_j = 0$, $i \neq j$, where $*$ is the Hadamard product, see [9],

(ii) $X_1 + X_2 + X_3 + X_4$ is a (1, −1) matrix,

(iii) $X_iX_j = X_jX_i$,

(iv) $X_1X_1^T + X_2X_2^T + X_3X_3^T + X_4X_4^T = xI_x$

T-matrices.

Statement 3. There exist T-matrices of order

(a) $1 + 2^a10^b26^c$, a, b, c natural numbers: Turyn [6],

(b) {1, 3,..., 59} Turyn [6],

(c) 61 Hunt [11].

In [9; p. 355] it is noted that Goethals and Seidel have given an array to construct Hadamard matrices of order $4m$ which requires four circulant (1, −1) matrices A, B, C, D of order m satisfying

$$AA^T + BB^T + CC^T + DD^T = 4mI_m, \tag{2}$$

viz.,

$$GS = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & -D^TR & C^TR \\ -CR & D^TR & A & -B^TR \\ -DR & -C^TR & B^TR & A \end{bmatrix}.$$

In this case R is found by using (1) and the cyclic group of order m.

Also in [9] it is noted that Wallis and Whiteman observed that A, B, C, D

only need be type 1. Hence if A, B, C, D are replaced by type 1 matrices of the form

$$X_1 \times X_2 \times \cdots \times X_n$$

where each X_i is type 1 and R is replaced by $R_1 \times R_2 \times \cdots \times R_n$, GS may still be used to form an Hadamard matrix (or Baumert–Hall array in Theorem 2 [9, p. 358]). Such an Hadamard matrix will be said to be of *Goethals–Seidel type.*

In this case the four $(1, -1)$ matrices A, B, C, D are called *Goethals–Seidel type matrices.*

THEOREM 2. (Cooper and Wallis). *If there exist T-matrices of order t there exists a Baumert–Hall array of order* $4t$.

The construction for the proof of Theorem 2 (see [9]) depends on the Goethals–Seidel array.

2. SOME USEFUL MATRICES

The following theorem shows how the Williamson construction (the B_i) and the Goethals-Seidel construction (the A_i) may be combined to construct Hadamard matrices.

THEOREM 3. *Suppose* A_i *and* B_i, $i = 1, 2, 3, 4$ *are type* 1 $(1, -1)$ *matrices of order a and b, respectively, which satisfy*

(i) $A_iA_j = A_jA_i \qquad i, j = 1, 2, 3, 4,$

(ii) $B_iB_j^T = B_jB_i^T \qquad i, j = 1, 2, 3, 4,$

(iii) $\sum_{i=1}^{4} (A_i \times B_i)(A_i \times B_i)^T = 4abI_{ab}$,

then, with R defined as above on the same abelian group as the A_i,

$$H = \begin{bmatrix} A_1 \times B_1 & A_2R \times B_2 & A_3R \times B_3 & A_4R \times B_4 \\ -A_2R \times B_2 & A_1 \times B_1 & A_4{}^TR \times B_4 & -A_3{}^TR \times B_3 \\ -A_3R \times B_3 & -A_4{}^TR \times B_4 & A_1 \times B_1 & A_2{}^TR \times B_2 \\ -A_4R \times B_4 & A_3{}^TR \times B_3 & -A_2{}^TR \times B_2 & A_1 \times B_1 \end{bmatrix},$$

is an Hadamard matrix of order $4ab$.

Proof. The verification is straightforward.

Henceforth we will call the matrices $A_i \times B_i$, $i = 1, 2, 3, 4$ of the theorem *F-matrices* and we will say H is an *Goethals–Seidel like Hadamard*

matrix. The A_i will be called the *GS-part* and the B_i the *W-part* of the F-matrix.

Matrices which are linear combinations of terms such as $A_i \times B_i$ and which can be used in H to form an Goethals-Seidel like Hadamard matrix will also be called F-matrices.

Clearly any Williamson type or Goethals-Seidel type matrix is also an F-matrix.

Let X_1, X_2, X_3, X_4 be four type 1 $(1, -1)$ matrices of order n (odd) with the properties

(i) $(X_i - I)^T = -(X_i - I)$, $i = 1, 2$,

(ii) $X_i^T = X_i$, $i = 3, 4$, and the diagonal elements are positive,

(iii) $X_iX_j = X_jX_i$,

(iv) $X_1X_1^T + X_2X_2^T + X_3X_3^T + X_4X_4^T = 4nI_n$.

Call such matrices *G-matrices*.

Multiplying both sides of (iv) by J shows G-matrices can only exist for orders n for which $4n = 1^2 + 1^2 + a^2 + b^2$, where a, b are odd integers. So, for example, they cannot exist for the following orders < 50: 11, 17, 29, 35, 39, 47.

G-matrices which are circulant exist for at least $n = 3, 5, 7, 9$. We give their first rows:

n	$4n$	
3	$1^2 + 1^2 + 1^2 + 3^2$	11–, 1–1, 1––, 111
5	$1^2 + 1^2 + 3^2 + 3^2$	111––, 1–1–1, 1––––, 1––––
7	$1^2 + 1^2 + 1^2 + 5^2$	1111–––, 11–1–1–, 1––11––, 1–––––––
9	$1^2 + 1^2 + 3^2 + 5^2$	1–11–1––1, 111–1–1––, 11–1111–1, 11––––––1

3. A Construction for F-Matrices Using G-Matrices

We now give some theorems showing how G-matrices may be used to construct F-matrices.

Theorem 4. *Let X_1, X_2, X_3, X_4 be G-matrices of order n. Suppose A, B, C are $(1, -1)$ matrices of order v which satisfy*

(i) *AB^T, AC^T, BC^T are symmetric,*

(ii) $AA^T + BB^T + (4n - 2)\,CC^T = 4nvI_v$.

Then

$$A_1 = I \times A + (X_1 - I) \times C, \qquad A_2 = I \times B + (X_2 - I) \times C,$$
$$A_3 = X_3 \times C, \qquad A_4 = X_4 \times C,$$

are F-matrices of order nv.

Proof. Clearly the A_i are $(1 -1)$, matrices with W-parts and GS-parts. Now

$$\sum_{i=1}^{4} A_i A_i^T = I_n \times (AA^T + BB^T + (4n - 2)\, CC^T),$$
$$= 4nvI_{nv},$$

so we have the result.

COROLLARY 5. *Suppose there exist G-matrices of order n. Further suppose there exist*

$$4n - \{v; 1 : k_1, 1 : k_2, (4n - 2) : k_3; k_1 + k_2 + (4n - 2)\, k_3 - nv\}$$

sds whose incidence matrices A, B, C satisfy AB^T, BC^T, AC^T all symmetric. Then there exist F-matrices of order nv.

COROLLARY 6. *Suppose there exist G-matrices of order n. Suppose there exists a symmetric Hadamard matrix of order (i) $2n + 2$, (ii) $4n$, (iii) $4n + 4$ and the form*

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & C & \\ 1 & & & \end{bmatrix}.$$

Then there exist F-matrices of order (i) $n(2n + 1)$, (ii) $n(4n - 1)$, (iii) $n(4n + 3)$, respectively.

Proof. Use (i) $A = J$, $B = J - 2I$, (ii) $A = J$, $B = C$, (iii) $A = J - 2I$, $B = C$, respectively, in the theorem.

COROLLARY 7. *Suppose there exist G-matrices of order n. Further suppose there exist (v, k, λ), (v, l, μ) and $(v, \frac{1}{2}(v - 1), \frac{1}{4}(v - 3))$ difference sets whose incidence matrices pairwise satisfy $XY^T = YX^t$. Then there exist F-matrices of order nv when $\lambda + \mu - l - k = n - \frac{1}{2}(v + 1)$.*

COROLLARY 8. *Suppose there exist G-matrices of order n. Further*

suppose there exists a $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ *difference set. Then there exist F-matrices of order.*

(i) $\frac{1}{2}v(v-1)$, $n = \frac{1}{2}(v-1)$;
(ii) $\frac{1}{4}v(v+1)$, $n = \frac{1}{4}(v+1)$;
(iii) $\frac{1}{4}v(v-3)$, $n = \frac{1}{4}(v-3)$; *respectively.*

Proof. Use the following difference sets in the previous corollary (i) J and K; (ii) J and Q; (iii) K and Q; respectively, where J represents the (v, v, v) difference set, K the $(v, v-1, v-2)$ difference set and Q the $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ difference set.

In particular, for $n = 5, 7, 9$ and (i), (ii), (iii), we have F-matrices of order 55, 95, 105, 115 171 189, 217, of which orders no Williamson type matrix was yet known for 105 and 171. It is also possible to find an F-matrix of order 351 using Corollary 6 (iii).

COROLLARY 9. *Suppose there exist G-matrices of order n. Further suppose there exists a* (v, k, λ) *difference set, D, and a* $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ *difference set defined on the same abelian group. Then there exist F-matrices of order*

(i) $v(\frac{1}{2}(v+1) - k + \lambda)$, $n = \frac{1}{2}(v+1) - k + \lambda$;
(ii) $v(\frac{1}{2}(v-1) - k + \lambda)$, $n = \frac{1}{2}(v-1) - k + \lambda$;
(iii) $v(\frac{1}{4}(v+1) - k + \lambda)$, $n = \frac{1}{4}(v+1) - k + \lambda$;

respectively.

Proof. With J, Q and K as in the proof of Corollary 8, use the following difference sets in Corollary 7,

(i) J and D; (ii) K and D; (iii) D and Q;

respectively.

The following theorem also gives F-matrices from G-matrices.

THEOREM 10. *Let* X_1, X_2, X_3, X_4 *be G-matrices of order n. Suppose* A, B, C, D *are* $(1, -1)$ *incidence matrices of* $4n - \{v; 1 : k, 1 : l, (2n-1) : \frac{1}{2}(v-1), (2n-1) : \frac{1}{2}(v-1); (n-1)v - 2n + k + l + 1\}$ *sds, and that* AC^T, AD^T, BC^T, BD^T, AB^T, CD^T *are symmetric. Then*

$$A_1 = I \times A + \tfrac{1}{2}(X_1 + X_2 - 2I) \times C + \tfrac{1}{2}(X_1 - X_2) \times D,$$
$$A_2 = I \times B + \tfrac{1}{2}(X_1 + X_2 - 2I) \times D + \tfrac{1}{2}(X_1 - X_2) \times -C,$$
$$A_3 = \tfrac{1}{2}(X_3 + X_4) \times C + \tfrac{1}{2}(X_3 - X_4) \times D$$
$$A_4 = \tfrac{1}{2}(X_3 + X_4) \times D + \tfrac{1}{2}(X_3 - X_4) \times -C$$

satisfy

$$\sum_{i=1}^{4} A_i A_i^T = 4nvI_{nv}\,.$$

That is A_1, A_2, A_3, A_4 are F-matrices of order nv.

Proof. We note $(X_1 + X_2 - 2I)^T = -(X_1 + X_2 - 2I)$, $(X_1 - X_2)^T = -(X_1 - X_2)$, $(X_3 \pm X_4)^T = (X_3 \pm X_4)$. Hence

$$\begin{aligned}\sum_{i=1}^{4} A_i A_i^T &= I \times (AA^T + BB^T) + (2n-1)I \times (CC^T + DD^T)\\ &= 4nvI_{nv}\,,\end{aligned}$$

and the A_i are F-matrices as required.

We note from [9] that a $(1, -1)$ matrix $I + N$ of order a is a symmetric conference matrix if $NN^T = (a-1)I$, $N^T = N$. These exist for orders $p + 1 \equiv 2 \pmod 4$, p a prime power and some other orders.

The existence of a symmetric conference matrix of order $v + 1$ is equivalent to the existence of $2 - \{v; \frac{1}{2}(v-1); \frac{1}{2}(v-3)\}$ sds and; of course, there exist (v, v, v) and $(v, v-1, v-2)$ difference sets in all groups. Similarly $2 - \{v; \frac{1}{2}(v-1); \frac{1}{2}(v-3)\}$ sds exist whenever $v + 1$ is the order of a symmetric Hadamard matrix. So we have

COROLLARY 11. *Suppose there exist G-matrices of order n. Suppose there exists a symmetric conference matrix or a symmetric Hadamard matrix of order $v + 1$. Then there exist F-matrices of order*

(i) $n(2n-1)$ *when* $v = 2n - 1$;

(ii) $n(2n+1)$ *when* $v = 2n + 1$;

(iii) $n(2n+3)$ *when* $v = 2n + 3$.

Proof. In the theorem use for (i) the (v, v, v) difference set twice; (ii) the (v, v, v) and $(v, v-1, v-2)$ difference set; (iii) the $(v, v-1\ v-2)$ difference set twice; respectively.

This corollary gives F-matrices of orders 45, 55, 65, 91, 105, 119, 153, 171, of these orders no Williamson matrix is yet known for 65, and 119.

COROLLARY 12. *Suppose there exist G-matrices of order n. Let p be a prime power. Then there exist F-matrices of order* (i) $n(2n-1)$ *when* $p = 2n - 1$; (ii) $n(2n+1)$ *when* $p = 2n + 1$; (iii) $n(2n+3)$ *when* $p = 2n + 3$,

This corollary also gives F-matrices of order 65, 105, 119, 153, 171. Another result is Corollary 13.

COROLLARY 13. *Suppose there exist G-matrices of order n. Further suppose there exists a* (v, k, λ) *difference set when* $v \equiv 1 (\text{mod } 4)$ *is a prime or a prime power. Then there exist F-matrices of order* (i) nv *where* $v = 2n - 1 + 2(k - \lambda)$; (ii) nv *where* $v = 2n + 1 + 2(k - \lambda)$; (iii) nv *where* $v = 2n - 1 + 4(k - \lambda)$.

Proof. When $v \equiv 1 (\text{mod } 4)$ is a prime power there exist

$$2 - \{v; \tfrac{1}{2}(v - 1); \tfrac{1}{2}(v - 3)\}$$

supplementary difference sets whose $(1, -1)$ type 1 incidence matrices C, D are symmetric. Let B be the type 2 $(1, -1)$ incidence matrix of the (v, k, λ) difference set. Then with (i) $A = J$, (ii) $A = J - 2I$, (iii) $A = B$ in the theorem we have the result.

Using (iii) and the existence of a (37, 9, 2) cyclic difference set we find an F-matrix of order 185 for which order no Williamson matrix is yet known.

4. CONSTRUCTION USING MATRICES OF WHITEMAN

THEOREM 14. *Suppose* X, Y *are* $(1, -1)$ *matrices of order* v *such that*

(i) $XY^T = YX^T$,

(ii) $XX^T = (v - 4m + 1) I + (4m - 1) J$,

(iii) $YY^T = (v + 1) I - J$.

Further suppose A, B, C, D *are four type* 1 $(1, -1)$ *matrices of order* m *which satisfy*

(a) A, B, C, D *pairwise commute*,

(b) $(A - I)^T = -(A - I)$,

(c) $AA^T + BB^T + CC^T + DD^T = 4mI_m$.

Then

$$A_1 = I \times X - (A - I) \times Y,$$

$$B_1 = B \times Y,$$

$$C_1 = C \times Y,$$

$$D_1 = D \times Y,$$

are F-matrices of order mv *and may be used to form an Goethals–Seidel like Hadamard matrix of order* $4mv$.

Proof. It is easy to check that

$$A_1A_1^T + B_1B_1^T + C_1C_1^T + D_1D_1^T = 4mvI_{mv}\,.$$

Then using Theorem 3 we have the result.

Now Whiteman (see [9, p. 331] and [10]) has shown such matrices A, B, C, D exist whenever $m = \frac{1}{4}(q+1)$, $q \equiv 3 \pmod 8$ a prime power. So we have

COROLLARY 15. *Suppose $q \equiv 3 \pmod 8$ is a prime power. Then there exist F-matrices of order $\frac{1}{4}q(q+1)$ and an Goethals–Seidel like Hadamard matrix of order $q(q+1)$.*

Proof. Use A, B, C, D to form an Hadamard matrix of order $q+1$. Obtain E as C was obtained in Corollary 6. Then with $X = J$, $Y = E$ in the theorem we have the result.

COROLLARY 16. *Suppose $q \equiv 3 \pmod 8$ is a prime power. Further suppose there exists a symmetric Hadamard matrix of order $q+5$. Then there exist F-matrices of order $\frac{1}{4}(q+1)(q+4)$ and an Goethals–Seidel like Hadamard matrix of order $(q+1)(q+4)$.*

Proof. Form E as before and put $X = J - 2I$, $Y = E$ in the theorem.

COROLLARY 17. *Suppose $q \equiv 3 \pmod 8$ is a prime power. Further suppose there exist (v, k, λ) and $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ difference sets defined on the same abelian (or cyclic) group and that $v - 4(k-\lambda) = q$. Then there exist F-matrices of order $\frac{1}{4}v(q+1)$ and an Goethals–Seidel like Hadamard matrix of order $(q+1)v$.*

Proof. Let X be the type 1 $(1, -1)$ incidence matrix of the (v, k, λ) difference set and let Y be the type 2 $(1, -1)$ incidence matrix of the $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ difference set in the theorem.

5. CONSTRUCTIONS USING THE RESULTS OF SZEKERES AND GOETHALS–SEIDEL

We use a construction of Szekeres [9; p. 321]. If $q = 4f+1$ (f odd) is a prime power and $C_0 = \{x^{4j} : j = 0, 1, \ldots, f-1\}$ where x is a generator of $GF(q)/\{0\}$, $C_i = x^iC_0$

$$C_0 \cup C_1 \quad \text{and} \quad C_0 \cup C_3\,,$$

are $2 - \{4f + 1; 2f; 2f - 1\}$ *sds* with the property that

$$a \in C_0 \cup C_1 \Rightarrow -a \notin C_0 \cup C_1, \quad b \in C_0 \cup C_3 \Rightarrow -b \notin C_0 \cup C_3, \quad a, b \neq 0.$$

Hence the type 1 $(1, -1)$ incidence matrices of these two sets satisfy

$$(X + I)^T = -(X + I), (Y + I)^T = -(Y + I), \tag{3}$$

$$XX^T + YY^T = (2q + 2)I - 2J. \tag{4}$$

Suppose N is a type 1 $(1, -1)$ matrix defined on the same group as $C_0 \cup C_1$ and $C_0 \cup C_3$ and such that

$$N^T = N, \qquad \text{(e.g., } J \text{ or } J - 2I). \tag{5}$$

Now as N, X, Y are all type 1 they commute (see [9]). Hence

$$\begin{aligned} NX^T &= N(-I + X + I)^T = -N + N(X + I)^T \\ &= -N - N(X + I) = -2N - XN \end{aligned}$$

and

$$NY^T = -2N - YN.$$

So

$$\begin{aligned} NX^T + XN^T &= -2N - XN + XN = -2N, \\ NY^T + YN^T &= -2N. \end{aligned} \tag{6}$$

LEMMA 18. *Suppose there exist four* $(1, -1)$ *matrices* M, N, X, Y *of order* v *satisfying*

(i) M, N, X, Y *pairwise commute,*

(ii) $MM^T + NN^T = 2(v - 2w + 1)I + 2(2w - 1)J,$

(iii) $XX^T + YY^T = 2(v + 1)I - 2J,$

(iv) $MX^T + XM^T - NY^T - YN^T = 0.$

Further suppose $I + R, S$ *are symmetric* $(1, -1)$ *matrices of order* w *which commute and for which*

$$RR^T + SS^T = (2w - 1)I,$$

then there exist F-matrices of order vw *and an Goethals–Seidel like Hadamard matrix of order* $4vw$.

Proof. Consider

$$A = I \times M + R \times X,$$
$$B = I \times N - R \times Y,$$
$$C = S \times X,$$
$$D = S \times Y.$$

Clearly A, B, C, D pairwise commute and have no W-part. Further

$$AA^T + BB^T + CC^T + DD^T = 4vwI_{vw}.$$

Hence A, B, C, D are F-matrices and may be used to form an Goethals-Seidel like Hadamard matrix of order $4vw$.

COROLLARY 19. *Let* $2w - 1 \equiv 1 \pmod 4$ *be a prime power. Suppose there exists a* (v, k, λ) *difference set with* $v - 4(k - \lambda) = 2w - 1$ *with a symmetric type* 1 $(1, -1)$ *incidence matrix* M. *Further suppose there exist* $2 - \{v; \frac{1}{2}(v - 1); \frac{1}{2}(v - 3)\}$ *sds with skew type* 1 $(1, -1)$ *incidence matrices. Then there exist F-matrices of order* vw.

Proof. $I + R$ and S of the theorem exist for order w where $2w - 1 \equiv 1 \pmod 4$ is a prime power. By (6) with $M = N$ the incidence matrices satisfy (ii) and (iv) of the lemma. By definition all the incidence matrices commute and (i) and (iii) of the lemma are satisfied. Hence we have the result.

COROLLARY 20. *Let* $2w - 1 \equiv 1 \pmod 4$ *and* $p = 4f + 1$ (f *odd*) *be prime powers. Suppose there exists a* (p, k, λ) *difference set with* $p - 4(k - \lambda) = 2w - 1$ *and a symmetric type* 1 $(1, -1)$ *incidence matrix. Then there exist F-matrices of order* pw.

Proof. Follows using the previous corollary and lemma, and the sds of Szekeres.

COROLLARY 21. *Let* $p \equiv 1 \pmod 4$ *be a prime power. Then there exist F-matrices of order* $\frac{1}{2}p(p + 1)$ *and when* $p - 4$ *is also a prime power* $\frac{1}{2}p(p - 3)$.

Proof. Use the (p, p, p) and $(p, p - 1, p - 2)$ difference sets.

This also gives F-matrices for orders 65 and 119, for which orders no Williamson type matrices are yet known. This result does not give new Hadamard matrices. In fact, Williamson type matrices exist for orders

$\frac{1}{2}p(p+1)$. Nevertheless, that there are F-matrices of order $\frac{1}{2}p(p-3)$ is of interest because of the structure of the resultant Hadamard matrix.

6. Final Remarks

It is the author's opinion that the Goethals–Seidel array and its adaption by Wallis and Whiteman for abelian groups is highly significant to the solution of the conjecture: *that there exists an Hadamard matrix of order $4t$ for all natural numbers t.* We list here those orders and classes for which F-matrices are known.

In the following list we use:

q $q \equiv 3 \pmod 8$, a prime power,

p a prime power,

g the order of a G-matrix

h the order of a symmetric Hadamard matrix.

(i)	w	w the order of a Williamson matrix; see Statement 2,
(ii)	t	t the order of a T-matrix; see Statement 3.
(iii)	$\frac{1}{4}(q+1)$	Whiteman.
(iv)	$\frac{1}{4}q(q+1)$	Corollary 15.
(v)	$\frac{1}{4}(q+1)(q+4)$	$q+5=h$; Corollary 16.
(vi)	$\frac{1}{4}v(q+1)$	(v, k, λ), where $v-4(k-\lambda)=q$, and $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ difference sets on the same abelian group must exist; Corollary 17.
(vii)	$\frac{1}{4}v(v+1)$	$\frac{1}{4}(v+1)=g$ and a $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ difference set exists.
(viii)	$\frac{1}{4}v(v-3)$	$\frac{1}{4}(v-3)=g$ and a $(v, \frac{1}{2}(v-1), \frac{1}{4}(v-3))$ difference set exists; Corollary 8.
(ix)	$\frac{1}{2}p(p+1)$	$g=\frac{1}{2}(p+1)$; Corollary 12, or $p \equiv 1 \pmod 4$; Corollary 21.
(x)	$\frac{1}{2}p(p-1)$	$g=\frac{1}{2}(p-1)$; Corollary 12.
(xi)	$\frac{1}{2}p(p-3)$	$g=\frac{1}{2}(p-3)$; Corollary 12. or $p \equiv 1 \pmod 4$; Corollary 21.
(xii)	$\frac{1}{2}(h-1)(h-2)$	$g=\frac{1}{2}(h-2)$; Corollary 6.
(xiii)	some others with more restrictive conditions.	

From this list we get (at least) F-matrices of order 119 which does not appear to arise in other ways.

We note that F-matrices exist for all but three odd numbers less than 100 (see Table 1).

TABLE 1[a]

Order	Class	Order	Class	Order	Class	Order	Class
1	*I*	27	*I*	51	II	77	*W*
3	*I*	29	*I*	53	*W*	79	*II*
5	*I*	31	*II*	55	*II*	81	*III*
7	*I*	33	*V*	57	*II*	83	*W*
9	*I*	35	*W*	59	*T*	85	*II*
11	*I*	37	*I*	61	*II*	87	*II*
13	*I*	39	*T*	63	*II*	89	
15	*I*	41	*II*	65	*T*	91	*II*
17	*I*	43	*I*	67		93	*VII*
19	*I*	45	*II*	69	*II*	95	*V*
21	*I*	47	*T*	71	*W*	97	*II*
23	*I*	49	*II*	73		99	*II*
25	*I*			75	*II*		

[a] Roman number–refers to Statement 2; *T*, a T-matrix exsists for this order (see Statement 3); *W*, Whiteman has formed a matrix of this order (see (iii) of this list).

REFERENCES

1. L. D. BAUMERT AND M. HALL, JR., A new construction for Hadamard matrices, *Bull. Amer. Math. Soc.* **71** (1965), 169–170.
2. L. D. BAUMERT AND M. HALL, JR., Hadamard matrices of Williamson type, *Math. Comp.* **19** (1965), 442–447.
3. D. C. HUNT AND J. WALLIS, Cyclotomy, Hadamard arrays and supplementary difference sets, *Proceedings of the Second Manitoba Conference on Numerical Mathematics*, (1972), 351–381.
4. M. PLOTKIN, Decomposition of Hadamard matrices, *J. Combinatorial Theory Ser. A* **12** (1972), 127–130.
5. T. STORER, "Cyclotomy and difference sets," *in* "Lectures in Advanced Mathematics," Markham, Chicago, Il, 1967.
6. R. J. TURYN, Computation of certain Hadamard matrices, *Notices Amer. Math. Soc.* **20** (1973), A-1.
7. J. S. Wallis, Construction of Williamson type matrices, to appear.

8. J. S. WALLIS, Williamson matrices of even order, Combinatorial Mathematics: Proceedings of the Second Australian Conference, *in* "Lecture Notes in Mathematics," Vol. 403, pp. 132–142, Springer-Verlag, Berlin, New York, 1974.
9. W. D. WALLIS, ANNE P. S., AND J. S. WALLIS, Combinatorics: Room squares, sum-free sets, Hadamard matrices, *in* "Lecture Notes in Mathematics," Vol. 292, Springer-Verlag, Berlin-Heidelberg-New York, 1972.
10. ALBERT LEON WHITEMAN, Skew-Hadamard matrices of Goethals-Seidel type, *Discrete Math.* **2** (1972), 397–405.
11. D. HUNT, private communication (1973).